Exposure and Breach of Information

Policy Type: Administrative
Responsible Office: Office of Technology Services, Division of Administration
Initial Policy Approved: 11/06/2014
Current Revision Approved: 01/08/2018

Policy Statement and Purpose

In the course of conducting its academic and research functions, Virginia Commonwealth University may collect, access, transmit and store sensitive information that is protected under various federal, state and industry regulations; this information is classified as Category I information under the university Data Classification Standard. To minimize financial and reputational risks caused by the loss of Category I information, university employees must safeguard this information and prevent any unauthorized access, loss, or theft of this information or devices containing such information.

Whenever Virginia Commonwealth University becomes aware of a suspected or actual exposure of its Category I information, specific action must be taken to work with university officials to determine a course of action to ensure compliance with federal state, and industry regulations in accordance with this policy.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

All university personnel who generate, collect, store, transmit, and process VCU Category I information should read and understand this policy.

Definitions

Affiliated Covered Entity (ACE)

VCU as a Health Insurance Portability and Accountability Act (HIPAA) hybrid entity and the VCU Health System (VCUHS) have designated themselves as an Affiliated Covered Entity (ACE), and VCU has designated certain VCU departments (or units) as required to comply with the HIPAA/HITECH standards.

Category I Information

Information protected under federal, state or industry regulations and/or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation.

Data Custodian

The data custodians can have both a business and/or technical role, though it is typically considered a business role. The data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

Data Steward

The data steward is a university director or equivalent employee who oversees the capture, maintenance and dissemination of data for a particular academic or business operation. The data steward is responsible for ensuring data quality, develop consistent data definitions, data sensitivity classifications, determining data aliases, developing standard calculations and derivations, defining security requirements, documenting all appropriate "business rules" and monitoring data quality within the source system and/or data warehouse. The data steward is also responsible for communicating data protection requirements to the data custodian; defining requirements for access to the data.

Information Security Incident (Incident)

An information security incident is an information security event that has jeopardized or has potentially jeopardized the confidentiality, integrity, and/or availability of the information system and/or the data contained in the information system. Information security incidents include but are not limited to

- Unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Information Exposure or Breach (Exposure)
Information exposure or breach refers to the unauthorized or improper access or disclosure of Category I information.

Notification
The communication of exposure or breach to the individuals affected by the information exposure or breach, as required by applicable state, federal, or industry regulations.

Contacts

VCU Office of Technology Services officially interprets this policy. Technology Services is responsible for obtaining approval for any revisions as required by the policy *Creating and Maintaining Policies and Procedures* through the appropriate governance structures. Please direct policy questions to Technology Services, Information Security Office (infosec@vcu.edu).

Policy Specifics and Procedures

The following specifics and procedures must be followed:

A. General Departmental Responsibilities

The department responsible for the suspected or actual exposure or breach of Category I information must inform the department head about the exposure or breach and work with the Information Security Office to determine appropriate action(s).

The department responsible for the suspected or actual exposure or breach has primary responsibility for addressing the exposure in accordance with the procedures provided in this policy. The department must work with data stewards to verify the confidentiality of the data and is responsible for working with the university Safety and Risk Management office, the Office of University Counsel, the university Information Security Office, and the Division of University Relations to develop an action plan that includes any communications, publicity, notifications and responses to affected individuals and others, and necessary remediation.

B. Handling of Information Exposures and Breach Notifications

The following procedure must be followed after a suspected exposure of information is discovered.

- Step 1. The person who discovers the suspected information exposure must notify the head of the department or designee responsible for the information without unreasonable delay.

- Step 2. Upon notification, the department head or designee of the department responsible for the information must notify the Information Security Office (infosec@vcu.edu) about the suspected information exposure without unreasonable delay. The department head or designee is responsible for determining whether the information in question is considered

Category I information.

- Step 3. The Information Security Office, in collaboration with the department responsible for the information, will coordinate an initial response to address the information exposure. The initial response may include the identification and analysis of the information security incident, the containment of the exposed information, eradication of any threats that may lead to further exposure, and the recovery and restoration of services.

- Step 4. The Information Security Office will coordinate the initial analysis and determine whether an actual exposure has likely occurred and notify the department of this determination.

- Step 5. If the information in question is considered Category I information and an actual exposure has likely occurred, the following steps will be followed. (Otherwise proceed to step 6)

  - a. The Information Security Office will notify the department responsible for the information, the university's Chief Information Officer, the Office of University Counsel, and appropriate vice president(s) that an exposure of Category I information has likely occurred.

  - b. The department responsible for the information will determine whether any of the following information has been exposed and notify the appropriate data steward(s) of the applicable information.

Information Type	Notification Recipient
HIPAA protected information	VCU ACE Chief Privacy Officer
HR and Payroll information	Assistant Vice President of Human Resources
Export Controlled Information	Director of Export Controls
FERPA Protected Educational Records	Registrar
Financial Records	University Controller
Other personally identifiable information	Information Security Office
Other Regulated or Protected Records	Information Security Office

  - c. The department responsible for the information will notify the university Safety and Risk Management office as well as the Division of University Relations.

  - d. The department responsible for the information, in combination with the appropriate data stewards, the university Safety and Risk Management office, the Division of University Relations, and the Office of University Counsel will determine whether an information exposure or breach notification is warranted pursuant to federal, state and industry regulations.

  - e. If it is determined that an information exposure or breach notification is warranted, the department responsible for the information exposure will work with the Safety and Risk Management office to notify the individuals affected by the information exposure.

- Step 6. The Information Security Office will record the incident, and assist the department responsible for the information with any additional remediation tasks related to the incident. The department responsible for the information will work with the Information Security Office to develop plans to prevent the reoccurrence of future incidents.

Forms

There are no forms associated with this policy.

Related Documents

1. VCU Data Classification Standard:

   https://ts.vcu.edu/media/technology-services/content-assets/documents/VCU_DataClassificationStandard_Final.pdf
2. Exposure and Breach of Information Handling Procedure Flow Chart:

   https://www.ts.vcu.edu/media/technology-services/content-assets/documents/DataBreachNotificationHandlingProcedures_08_2017.pdf

3. Code of Virginia: Breach of Personal Information (§ 18.2-186.6):

   http://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

4. Code of Virginia: Breach of Medical Information Notification (§ 32.1-127.1:05.):

   http://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/

5. Export Administration Regulation (EAR):

   https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

6. Family Educational Rights and Privacy Act (FERPA):

   https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

7. Graham-Leach-Bliley Act (GLBA):

   https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

8. Health Insurance Portability and Accountability Act (HIPAA):

   https://www.hhs.gov/hipaa/index.html

9. Health Information Technology for Economic and Clinical Health Act (HITECH):

   https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations

10. International Traffic of Arms Regulation:

    http://pmddtc.state.gov/regulations_laws/itar.html

11. Code of Virginia: Breach of Personal Information (§ 18.2-186.6):

    http://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

12. Code of Virginia: Breach of Medical Information Notification (§ 32.1-127.1:05.):

    http://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/

13. Virginia DHRM Personnel Records Disclosure Policy (Policy number 6.05):

    http://web1.dhrm.virginia.gov/itech/hrpolicy/pol6_05.html

14. Virginia DHRM Personnel Records Management Policy (Policy Number 6.10):

    http://www.dhrm.virginia.gov/docs/default
    source/hrpolicy/pol6_10personnelrecordsmanagement.pdf?sfvrsn=2

15. VCU Information Technology Policy Framework

    https://ts.vcu.edu/askit/policies-and-publications/information-technology-policies-standards-baselines--guidelines/

16. VCU Policy: *Computer Network and Resources Use*

    https://policy.vcu.edu/sites/default/files/Computer%20and%20Network%20Resources%20Use.pdf

17. VCU Policy: *Information Security*

    https://policy.vcu.edu/sites/default/files/Information Security.pdf

18. VCU Standard: *Incident Response Standard*

    https://ts.vcu.edu/media/technology-services/content-assets/ts-groups/information-security/IncidentResponseStandard-2016.1.pdf

Revision History

This policy supersedes the following archived policies:

11/6/2014 *Exposure and Breach of Information*

FAQ

1. What is considered Category I information?

Information containing the following data elements are considered Category I information. For a full explanation on information and data classification, please see the VCU Data Classification Standard.

- First name or first initial and last name in combination with and linked to any one or more of:
    - Social Security Number
    - Driver's license number or state issued ID number in lieu of driver's license number
    - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts
    - Any information related to an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional
    - An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records
- Protected Health Information as defined by HIPAA
- Student Financial AID information protected under Gramm-Leach-Bliley Act
- Student Educational Records as defined by FERPA (Excluding Directory Information)
- Export controlled information regulated under ITAR, EAR
- Commonwealth of Virginia Identification Number (BES ID)
- Employee and personnel records protected by Virginia Department of Human Resources Management policies
- Other regulated information that if lost or stolen may require breach notifications and lead to fines

2. Are there any examples of information security incidents?

Yes, examples of information security incidents may include but are not limited to:

- A lost or stolen laptop, smart phone, thumb drive or other electronic storage device that is unencrypted
- Successful hacking and intrusion against an IT system
- Loss or theft of paper records
- Loss or theft of user account credentials that allow an individual to access protected data without authorization
- Intentional or unintentional public posting of sensitive information on the internet
- Internal fraud involving the sale or trafficking of confidential and regulated information
- Posting of sensitive information on publicly accessible electronic or paper media
- Unauthorized interception of unencrypted information in transmission